OBJECTIVES

After completing this chapter, you should be able to:

1. Outline the general strategies adopted in electronic commerce legislation to ensure business certainty in the online environment.
3. State the considerations involved to ensure successful contract formation in electronic commerce.
4. Discuss the contractual issues specific to automated electronic commerce and the legislative method for correcting keystroke errors.
5. Explain the importance of authentication in online business transactions.
6. Describe how public key cryptography can be used to create electronic signatures.
7. Outline the business problems arising from the domain name system.
8. Discuss the jurisdictional implications of transacting in a global medium and how to minimize exposure to liability online.
9. Describe how an online business can shield itself from intermediary liability.
10. Explain how consumer protection principles can be used to promote the reputation of a business, generate goodwill, and build trusting relationships.
Knowledge-based businesses can distribute their products through various technological channels. Therefore, they are well positioned to participate in **electronic commerce**. **Electronic commerce** refers to technology-mediated business transactions. These take place across a network and usually involve the transportation of goods, services, or information—either physically or digitally—from one place to another. It is tempting to think of the Internet when one thinks of electronic commerce, but the definition is actually much broader. It also includes, for instance, a transaction that occurs between a customer and an automated bank machine.

Electronic commerce has a number of benefits. Once a system is in place, transactions become easy and affordable. Technology allows a business to reach more customers, in more places. It allows contracts to be performed more quickly. And it can reduce the expenses associated with marketing products and creating contracts. However, electronic commerce also has its costs. One such cost is uncertainty.¹

One significant source of uncertainty is the law. The basic rules of commercial law were developed many years ago, when people usually dealt face to face. Not surprisingly, those rules are often poorly suited to transactions that are conducted over a network. As a matter of risk management, a business that is involved in electronic commerce must be aware of potential problems. This chapter therefore examines how the law has responded to technological changes in the business world. We begin with a survey of recent legislation that regulates electronic commerce. We then discuss how enforceable contracts can be created electronically and explore some specific issues that can arise from electronic commerce, including the use of domain names and the possibility of imposing liability in Internet-related services. We conclude with an outline of the fundamental principles guiding consumer protection in the sometimes dangerous online environment.

**ELECTRONIC COMMERCE LEGISLATION**

A defining feature of electronic commerce is that it is global—it allows business to be done around the world. It is therefore desirable to have consistent laws from place to place. If every jurisdiction had a different set of rules, it would be impossible to achieve certainty in the electronic business world. As a result, the United Nations Commission on International Trade Law (UNCITRAL) encouraged countries to create uniform legislation based on a single model—a Model Law on Electronic Commerce.² That model law is not really a law. It does not create rights, powers, obligations, or immunities. It merely provides a *model* for the creation of a consistent set of laws. Ultimately, it is up to each government to decide how much of the model to adopt. Note that the model law is not intended to create entirely new types of legal relationships. Instead, its goal is to remove barriers that technology may impose upon the creation of traditional commercial relationships.

**Canada’s Uniform Electronic Commerce Act**

Because our Constitution states that commerce is generally a provincial matter, electronic commerce legislation has been enacted on a province-by-province basis.

---

¹ The effects of uncertainty have been felt in the marketplace. That became evident at the outset of the new millennium, when many of the promises of the so-called *dot-com revolution* were disappointed.

basis. Still, the co-ordination of these rules was inspired on a national level. The strategy was similar to the international approach. A special working group of the Uniform Law Conference of Canada created its own model law—the Uniform Electronic Commerce Act (UECA).\textsuperscript{3} Like UNCITRAL's model law, UECA has no legal force, but it has formed the basis for most electronic commerce laws in Canada. Some provinces have adopted all of it; others have adopted specific parts. Because of its significance, we will examine UECA's most important provisions in detail. In particular, we will consider:\textsuperscript{4}

- its scope
- the role of consent
- the notion of a functional equivalent
- the rules pertaining to electronic contracts
- the rules pertaining to sending and receiving electronic documents
- the treatment of government documents

**Scope**

UECA has a broad scope. Rather than listing all of the transactions to which it applies, it lists those to which it does not apply. For instance, it follows UNCITRAL's model law by specifically excluding wills and dealings in land. Those sorts of arrangement are still governed by the traditional rules. The list of exclusions differs, however, between jurisdictions. To manage risk, it is therefore important for a business involved with electronic commerce to know which exclusions apply in every jurisdiction in which it does business.

**Consent**

UECA does not require a business to use or accept electronic documents. It is meant only to facilitate electronic commerce for those people who choose to engage in it. It is important to realize, however, that your consent may be express or implied. The courts may decide that you consented to use UECA if you behave in a way that supports that inference.

**Functional Equivalence**

As we saw in Chapters 5 and 14, some types of contract traditionally were enforceable only if they were in writing. That is still true. UECA, however, recognizes that the writing requirement can sometimes be satisfied through functional equivalence. Functional equivalence identifies the essential purpose of a traditional rule and indicates how that purpose can be accomplished electronically.

For example, some statutes that regulate the enforcement of contractual terms require certain documents to be signed. That signature is intended to demonstrate the signer's willingness to be bound by the terms. However, that same purpose may be achieved through the click of a mouse. For instance, a dialogue box may appear on a computer screen that contains a box that says, "I accept these terms." Clicking on that box may be the functional equivalent of signing a document.\textsuperscript{5}


\textsuperscript{5} There are many other examples. The essential function of writing is memory, which can also be satisfied by electronic information, as long as it is accessible for future reference.
Electronic Contracts

*UECA* does more than permit functional equivalents. It even allows transactions to be achieved, without human intervention, by computer programs. For instance, contracts may be created by shopping bots (as we saw in Business Law in Action 2.2) and other automated electronic devices.

Sending and Receiving Electronic Documents

*UECA* also facilitates electronic commerce by removing uncertainty about where and when a message is sent or received.

A message is deemed to be sent from the sender’s place of business and received at the recipient’s place of business. Suppose that your place of business is in Alberta, but that you send a message through your Internet server in Manitoba, while you are travelling in the Yukon. It can plausibly be said that your message was sent from any one of three places. *UECA* therefore eliminates the uncertainty and promotes commerce by consistently choosing one of those possibilities.

*UECA* also contains clear rules that determine when a message is sent or received. A message is deemed to be sent when it leaves the sender’s control. Consequently, once you push a button and can no longer stop the message from being sent, that message is considered sent, even if it is never received. A message is deemed received when it reaches an information system in the control of the person to whom it is sent. That rule can be tough on recipients because they can be on the hook even if they never actually read the messages. However, a recipient can claim that a particular message was never received by proving, for instance, that it could not be downloaded from the server. The best way for a business to avoid disputes about the transmission of its messages is to either require acknowledgment or invoke a system of automated confirmation.

Note that *UECA*’s provisions do not change the common law rules regarding the communication of acceptance. As we saw in Chapter 2, contractual acceptance must be communicated to be effective. Furthermore, the time and the place of the acceptance depend upon the medium of communication. *UECA* has avoided the issue of instantaneous versus non-instantaneous communication, recognizing that the decision about whether to treat a particular electronic transmission as similar to a phone call or first-class mail depends upon the circumstances and must be determined on a case-by-case basis.

Note that the rules eliminating uncertainty about where and when a message is sent or received are merely default rules. In other words, parties can choose to adopt their own rules by mutual consent.

Government Documents

Governments electronically exchange an enormous amount of information with businesses and citizens and will do so even more as Canada’s Government Online and similar provincial initiatives are fully implemented. *UECA* therefore contains a number of provisions regarding electronic documents that are sent to government. For instance, some provisions protect governments from being swamped by electronic documents that arrive in various incompatible formats. A government can specify the formats that it is willing to accept.

---

6. The rules are more complicated if a company has several places of business or no place of business.

7. For the purposes of *UECA*, the term “government” does not include Crown corporations, but it may include municipalities, if the provincial or territorial legislature so decides.

8. Some jurisdictions, including Ontario, Nova Scotia, and the Yukon have adopted those provisions. Others, such as British Columbia and New Brunswick, have not.
Provincial Electronic Commerce Legislation

UECA is a model for provincial electronic commerce legislation. Many provinces have adopted that model entirely or with minor variations. Others have attempted to overcome the same problems by other means. Although it is impossible to provide a detailed comparison of each jurisdiction’s approach, we can mention a few important differences.

The most substantial differences occur in New Brunswick and Quebec. For example, unlike most of its counterparts, the New Brunswick legislation does not regulate the process of offer and acceptance. And the Quebec legislation is much more extensive than its counterparts. For instance, it contains a number of detailed provisions regarding the consultation and transmission of documents that have legal implications for third parties, like online service providers. As a matter of risk management, the lesson is clear. While UECA has provided a model for electronic commerce statutes, there are occasional substantial differences between jurisdictions. Businesses that are not confined to a single province or territory should consult the relevant legislation to avoid difficulties.

CONTRACTING ONLINE

Although UECA and the statutes that it inspired remove many sources of uncertainty about online commerce, a number of difficulties remain. In this section we will look at three issues:
- contract formation
- automated electronic commerce
- authentication and security

Contract Formation

The fact that commerce is conducted electronically creates certain problems for traditional rules governing the formation of contract. Some pertain to shrink-wraps, click-wraps, and web-wraps, while others pertain to the basic process of offer and acceptance.

Shrink-wraps, Click-wraps, and Web-wraps

A shrink-wrap licence occurs in the context of mass-marketed software. The software is placed in a package that is wrapped in clear cellophane. Underneath the cellophane is a card, which states the rules that are attached to the use of the software. That card also informs consumers that, by removing the

---


cellophane, they are agreeing to abide by those rules—they can use the software, but they must honour the terms of the licence that has been created.\footnote{A licence is simply permission to act in a way that would normally be prohibited. In this case, the licence allows the consumer to use the manufacturer's software.}

The same basic process can be used for online commerce. A click-wrap licence is created when a person agrees to accept the terms of an online contract by clicking a mouse or touching an icon that says, “I accept.” A click-wrap licence can be any licensing agreement triggered by the click of a mouse. A web-wrap licence is similar, but more specific. A web-wrap licence is triggered by some form of online interaction. For example, while viewing a document online, you try to download or install software, or order goods or services. A window pops up that (i) contains the terms of a contract, (ii) asks you to read those terms, and (iii) tells you to click on one box to accept those terms or on another to reject them. If you click on the first box, you may be bound by a contract. Canadian courts have said that, when properly constructed, such agreements are “afforded the same sanctity that must be given to any agreement in writing.”\footnote{Rudder v Microsoft (1999) 47 CCLT (2d) 168 at para 17 (Ont SCJ).} Case Brief 17.1 illustrates this.

**CASE BRIEF 17.1**

**Rudder v Microsoft (1999) 47 CCLT (2d) 168 (Ont SCJ)**

Microsoft Network (MSN) provides online information services to members of its network. The plaintiffs were two Canadian law students who had entered into an online contract to receive MSN’s services. They started a lawsuit in Ontario against MSN when they believed that they had been improperly charged for certain services.

MSN pointed to a provision in the online contract that it had created with the plaintiffs. That provision required any disputes to be resolved through the courts in the State of Washington. MSN therefore said that the case could not be heard in Canada. In response, the plaintiffs argued that they had not noticed the “forum selection clause” and argued that the clause should be treated as “fine print,” since only a portion of the agreement was on screen at any given time.

The court held that the plaintiffs had agreed to obey the terms of the online contract when they clicked on the button that said, “I agree.” The court then rejected the argument that any terms not wholly in view must be understood as fine print. Such a claim, it held, was no different from saying that only the terms and conditions that appear on the signature page of a printed document should apply. The court also said that ignorance of the relevant term was no excuse since MSN’s agreement required potential members to view its terms on two occasions and signify acceptance on each occasion. In fact, the second display of the terms advised users that, “If you click ‘I agree’ without reading the membership agreement, you are still agreeing to be bound by all of the terms...without limitation.”

The court in Rudder v Microsoft rejected the plaintiffs’ argument partly because those arguments would “lead to chaos in the marketplace, render inefficient electronic commerce and undermine the integrity of any agreement entered into through this medium.” That decision recognizes the interests of businesses that engage in electronic commerce. However, the court also stressed the fact that click-wrap and web-wrap agreements are similar to traditional contracts in one important way—the terms of a contract are effective only if they are sufficiently brought to the parties’ attention. To manage risk, therefore, those terms should be as conspicuous as possible. If terms are hidden in a remote hyperlink or camouflaged in unusual fonts or footnotes, they may not be effective.

\footnote{That was traditionally true in the “ticket cases,” which were discussed in Chapter 4.}
Offer and Acceptance

Online contracts also create challenges for the traditional rules regarding offer and acceptance. For instance, if a Web site proposes a contract, does it create an *offer* or merely an *invitation to treat*? As we saw in Chapter 2, if an offer is made to the world at large, it may be accepted by many people. If so, the offeror is required to fulfill many contracts, even if it really wanted to create only one. As a matter of risk management, you should design your Web site so that it extends only an invitation to treat. You should require each customer to place an order, that is, make offers, that you are free to accept or reject.

Electronic commerce also raises issues about the communication of acceptance. Chapter 2 explained how the traditional common law rule depends upon whether the communication is instantaneous (like a telephone call) or non-instantaneous (like a letter). Most jurisdictions in Canada have followed UECA by enacting legislation that deems when and where electronic communications are sent and received. However, most of those statutes do not specify whether particular forms of communication are instantaneous or non-instantaneous. Businesses should prepare for the possibility that an e-mail may be lost or delayed in cyberspace. The safest route is to use various means of communication. For example, if an e-mail message is important, it might be backed up by a fax, regular letter, or telephone call. While electronic commerce is generally intended to avoid that inconvenience, it is still sometimes better to have a back-up plan. The extra effort may save many years and much money in litigation. Admittedly, such safety mechanisms may become impossible as transactions become completely automated.

Automated Electronic Commerce

As commercial transactions veer off traditional paths and swerve onto the information superhighway, the cornerstone of traditional contract theory, the notion of *consensus ad idem* (a “meeting of the minds”) becomes more difficult to apply. As businesses move further into electronic environments, commercial transactions will no longer be created and performed exclusively by humans. Many transactions will be initiated and completed by computer software programs. These automated transactions will not easily fit within traditional notions of contract. In fact, the point of developing technologies that automate electronic commerce is to allow transactions to take place without any need for humans to review or even be aware of particular transactions. And significantly, unlike the technology that is currently used in things like vending machines and mechanical parking attendants, fully automated forms of electronic commerce will not simply act in predetermined ways by dispensing candy or parking stubs on demand. They will act intelligently and somewhat independently of their human creators. For example, when linked to a warehouse computer, they may detect a shortage of stock and order supplies without being instructed to do so by a human.

Most Canadian electronic commerce statutes allow contracts to be created by automated electronic devices.\(^\text{14}\) However, while enforceable contracts can be created in that way, it may be dangerous to rely on such systems. Most of the statutes also say that transactions are unenforceable when purchasers make a *keystroke error* when dealing with an automated system. A *keystroke error* occurs when a person mistakenly hits a wrong button or key. For instance, you

---

\(^{14}\) Section 21 of UECA states: "A contract may be formed by the interaction of an electronic agent and a natural person or by the interaction of electronic agents."
may order 1000 items instead of 100, or you may hit the “I agree” button instead of the “I decline” button. An automated system normally cannot recognize subsequent messages that you send in an attempt to correct a mistake. It will simply fill your order as originally received. The legislation may allow you to escape the consequences of your error in certain circumstances. Basically, you must prove that: (i) the automated system did not provide an opportunity to prevent or correct the error; (ii) you notified the other party of the error as soon as possible, (iii) you took reasonable steps to return any benefit that you received under the transaction, and (iv) you have not received any other material benefit from the transaction. An online business can avoid those sorts of situations by creating an automated mechanism to correct such errors. The simplest tactic is to require the purchaser to confirm the order by repeating the important steps (for instance, by retyping the number of items that it wants to receive).

**Authentication**

In our earlier discussion of functional equivalents, we saw that a signature can serve the important goal of demonstrating a person’s willingness to be bound to a contract. But a signature can also provide an authenticating function. An authenticating function identifies the signatory and ties that person to the document. In many situations, contractual parties are not concerned about each other’s identity. If you buy a bowl of matzo ball soup from my deli, I do not care who you are, and you do not care who I am. However, a party’s identity is often important, especially in electronic commerce. Suppose that we create a contract online that requires you to pay $10 000 and that requires me to deliver an Internet server. Without some form of authentication, either you will have to pay and trust me to send the server, or I will have to send the server and trust you to pay. Although people often do business on the basis of trust, it is a dangerous practice, especially among strangers. Risk management therefore suggests the need for authentication. At least one of us has to be satisfied that the other can be trusted. Electronic signatures can be used for that purpose.

**Electronic Signatures**

An electronic signature is electronic information that people can use to identify themselves. The process in which a person uses an electronic signature usually involves two components:

- a trusted third party known as a certification authority
- technology known as public key cryptography

Although the process is complicated, we can briefly describe it.

**Certification Authorities** An electronic signature is reliable if it is used in conjunction with a trusted third party. A trusted third party is a person whom both contractual parties can trust. While I may not be willing to rely on information that I receive from you, I may be willing to rely on that same information if it has been verified by someone whom I know and trust. That trusted third party therefore uses a digital certificate to verify the identity of the person who provided the electronic signature. A digital certificate is an electronic document that authenticates the identity of a particular person. In many ways, it is like an electronic credit card—it is used to establish your credentials when doing business online. A trusted third party who provides that sort of certificate is known as a certification authority.
Note that a certification authority need not be limited to verifying a person’s identity for electronic signatures in online contracts. Digital certificates can also be used to certify a person’s age, whether that person holds a licence to use certain online services, whether a person’s level of security clearance authorizes access to an information system, and so on. These sorts of certification are now possible through the development of a special type of trusted third party system called a public key infrastructure. A public key infrastructure (PKI) is a set of policies and procedures that provides a high level of security and therefore allows businesses, consumers, governments, and courts to trust the information that they protect.\textsuperscript{15}

PKI is based on cryptography. Cryptography is the science of encryption and decryption. Julius Caesar originally popularized it. Since he did not trust his messengers with the information that he sent to his governors and officers, he encrypted his messages. Encryption is the coding of plaintext into an unreadable form called ciphertext so that it cannot be understood by those who do not have the relevant code. Caesar used a simple system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. Authorized recipients of his messages were provided with the code for decrypting them. Decryption is the process of converting ciphertext back into its original form so that it can be understood.

Caesar’s system relied on the creation of a private code (nowadays referred to as a private key) that was intended to be shared only amongst confidants. That system had an obvious weakness. If the key ever fell into the wrong hands, the messages could be decrypted by unauthorized people. For that reason, Internet users prefer public key cryptography. In public key cryptography, two keys are created: one is private, the other is public. Although those two keys are distinct, they are created in a way that allows a message that was encrypted by your public key to be decrypted with your private key and vice versa. Because two keys are required—one to encrypt, the other to decrypt—no one has to share their private key with anyone else. The public key is made available online to the public at large. It allows anyone who possesses it to send encrypted information to you. The private key, however, is kept secret and remains solely in your custody. This system, when used in conjunction with a certification authority, ensures that no one else can read the encrypted messages that you send or receive.

A similar procedure can be used to create electronic signatures, although the key’s functions are reversed. An electronic signature is the ciphertext that is created by an encrypted message. If you sign your message with your private signature key, I can decrypt that signature with your public signature key and compare it to the message. If they are identical, I can reasonably assume that the message was from you, since presumably you are the only one in possession of your private key. Thus, decrypting an electronic signature using a public key is one way to verify an electronic signature. Concept Summary 17.1 reviews the uses of PKI.

\textsuperscript{15} American Bar Association draft Public Key Infrastructure Assessment Guidelines: <www.abanet.org/scitech/ec/isc>.
Concept Summary 17.1

Uses of PKI in Electronic Commerce

- to send and receive confidential messages
- to create electronic signatures
- to verify another’s electronic signature
- to validate digital certificates

**FIGURE 17.1** Asymmetrical Cryptography or Encryption Is a Dual Key System

The sender, A, encrypts an e-mail “I am sending you a secret message” with B’s public key. The message is transformed into a string of 1s and 0s. The recipient of A’s message, B, uses her private key to decode the string of 10011100111001 as “I am sending you a secret message.” Likewise, B could use A’s public key to send an encrypted message to A.

Information Security

Although PKI systems are very useful, they have dramatic implications for privacy. As one author stated, “[t]he current approach to digital certificates and Public Key Infrastructures ignores the privacy rights of individuals, groups, and organizations. Digital certificates can be followed, traced, and linked instantaneously as they move around. Unless drastic measures are taken, individuals will soon be forced to communicate and transact in what could be the most pervasive electronic surveillance system ever built.”

Ethical Perspective 17.1 discusses another side of the privacy question.

---

Since many corporations connect their internal networks to the Internet, most business people view the privacy concerns associated with PKI as a necessary evil. Similarly, while the Internet’s greatest virtue is said to be its open-access, accessibility also creates the risk of invasion from malicious hackers, hacktivists, cyber-criminals, cyber-terrorists, and industrial spies. Online intruders can steal information-based assets; dilute corporate brands; cause critical infrastructure failures, service breaks and system failures; and scare away customers. Consider Case Brief 17.2.

Questions for Discussion
1. Would you say that Dale and Bruce have transgressed PIPEDA? Why?
2. How would you respond to an argument by Dale and Bruce that they are simply making more accessible information that is already available to the public?
3. What moral considerations should Dale and Bruce have taken into account before they decided to stream cellular phone conversations?

Since many corporations connect their internal networks to the Internet, most business people view the privacy concerns associated with PKI as a necessary evil. Similarly, while the Internet’s greatest virtue is said to be its open-access, accessibility also creates the risk of invasion from malicious hackers, hacktivists, cyber-criminals, cyber-terrorists, and industrial spies. Online intruders can steal information-based assets; dilute corporate brands; cause critical infrastructure failures, service breaks and system failures; and scare away customers. Consider Case Brief 17.2.

Questions for Discussion
1. Would you say that Dale and Bruce have transgressed PIPEDA? Why?
2. How would you respond to an argument by Dale and Bruce that they are simply making more accessible information that is already available to the public?
3. What moral considerations should Dale and Bruce have taken into account before they decided to stream cellular phone conversations?

Since many corporations connect their internal networks to the Internet, most business people view the privacy concerns associated with PKI as a necessary evil. Similarly, while the Internet’s greatest virtue is said to be its open-access, accessibility also creates the risk of invasion from malicious hackers, hacktivists, cyber-criminals, cyber-terrorists, and industrial spies. Online intruders can steal information-based assets; dilute corporate brands; cause critical infrastructure failures, service breaks and system failures; and scare away customers. Consider Case Brief 17.2.

Questions for Discussion
1. Would you say that Dale and Bruce have transgressed PIPEDA? Why?
2. How would you respond to an argument by Dale and Bruce that they are simply making more accessible information that is already available to the public?
3. What moral considerations should Dale and Bruce have taken into account before they decided to stream cellular phone conversations?
As the Mafiaboy case illustrates, PKI and other security measures are crucial to the success of Internet commerce. One expert has said that security is “what transforms the Internet from an academic curiosity into a serious business tool.” Security protects corporate assets from external threats. Information security can be used to protect your business against the threat of things like tampering, interception, worms, viruses, and logic bombs. Information security is a combination of communications security and computer security. Communications security protects information while it is transmitted from one system to another. Computer security protects information within a computer system.

Hardware and software are not the only means of protection. A comprehensive information security system must include other forms of control, including strict workplace policies and personnel security. Businesses can also protect themselves by using the law as a deterrent, by informing those with access to information systems that they will be punished (perhaps by the loss of Internet privileges or even summary dismissal) if they engage in illegal activities like online gambling, possessing child pornography, sexual harassment, and fraud.

Businesses should also publicize that the Criminal Code of Canada contains a number of provisions designed to prevent security breaches.

- Section 342.1 prohibits the unauthorized use of a computer, including theft of computer services, breaches of privacy, and trafficking in computer passwords.
- Section 430 (1.1) prohibits computer mischief that: (i) destroys or alters data, (ii) renders data meaningless, useless or ineffective, (iii) obstructs, interrupts or interferes with the lawful use of data, or (iv) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.
- Sections 183 and 184 prohibit the interception of private communications. The definition of “private communications” is quite broad, and includes any telecommunication made in Canada or intended to be received in Canada. Business managers charged with information security will be relieved to know that an exception exists where it is reasonable to expect that the communication may be intercepted, as in the employment context.

Businesses can use contract law to protect themselves against some security risks. As we saw in Chapter 16, they can adopt confidentiality agreements. Likewise, they should also create, publicize, and enforce against all company employees an Internet use policy. That policy should include provisions governing: (i) the use, disclosure, and return of confidential information, (ii) use of the Internet, and (iii) permission to monitor employee communications.

Businesses can also reduce some security risks by outsourcing to security providers, including certification authorities. By outsourcing, the security provider or its insurer assumes some of the risk of maintaining security.

---

DOMA IN NAMES

We have examined the core contractual aspects of electronic commerce. Now we will investigate other legal issues that can arise as a business migrates to the online terrain. Although a key benefit of electronic commerce is that geography becomes less important, the marketing slogan—location, location, location—is still relevant online. Perhaps the most important real estate in cyber-space is the domain name. A domain name locates an organization on the Internet. For example, by entering www.pearsoned.ca into an Internet browser or search engine, you will locate the Internet address for the company Pearson Education Canada, the publisher of this book.23 Because of the enormous number of domains on the Internet, several organizations regulate their acquisition and use.24

In the world of real estate, a person may buy a piece of land with a view to reselling it at a profit. The same sort of activity can happen on the Internet. A cybersquatter purchases a potentially valuable domain name with the intention of later selling it to the highest bidder. For example, some cybersquatters reserve domain names for common English words (like drugstore.com or furniture.com) to resell them to companies that are interested in dealing with the relevant products online. If no one claims a prior right to a particular domain name, the first person to register it becomes the owner and has the right to resell it. Problems arise, however, when a domain is not merely a common word but rather a name that someone else asserts some sort of proprietary interest in. Although the regulating authorities have received complaints about thousands of domain names, the disputes usually fall into three groups.

- A person may innocently, or with some justification, register a domain name that is later disputed. For example, if your new-born nephew is named Ed Pearson, you might register the domain www.pearsoned.ca and post pictures of him at that address. You may receive a complaint from Pearson Education Canada, which holds a proprietary interest in that name.

- A person may register a domain name that resembles a trademark to which both parties claim a commercial right. For example, if you hold the US trademark Pearson International®, you may register www.pearsoninternational.ca. If so, you may receive a complaint from the Greater Toronto Airport Authority, which believes that, as operator of Pearson International Airport and holder of a similar registered Canadian mark, it has a stronger claim to that domain name.

- A person may register a domain name in which it has no commercial rights. For example, you might try to be the first to register www.pearsoned.ca, either to prevent Pearson Education Canada from using it or to offer it for sale to Pearson’s competitors at a price far exceeding its cost.

Sometimes, cybersquatters feel that they are morally justified in taking a domain name. Consider the case in Business Law in Action 17.1.

---

23. Like many other international companies, Pearson Education has registered several other domain names, such as <www.pearsoneducation.com>.

24. For instance, dot-ca (as in <www.pearsoned.ca>) is administered by the Canadian Internet Registry Authority (CIRA) <www.cira.ca>.
In some circumstances, the parties are entitled to litigate such matters. However, litigation requires a great deal of time and money to decide cases in the courts. Furthermore, because cybersquatting is a global activity, it is often difficult to decide which court should hear the matter. As a result, the bodies that regulate domain names have adopted procedures to resolve disputes primarily through arbitration. As we discussed in Chapter 1, arbitration is a form of alternative dispute resolution (or ADR) that allows the parties to settle their argument without a court order. As a matter of risk management, the best strategy is to avoid difficulties altogether. While that is not always possible, businesses can take steps to minimize the potential for domain name disputes. For instance, a business manager who is responsible for a company's e-commerce development should register bona fide trademarks and business names as early as possible to avoid being held hostage by a cybersquatter. Note that even a registered trademark will not guarantee your business a proprietary interest in a particular domain name. Arbitrators have demonstrated a willingness to weigh the public interest in free speech and fair use against the rights of trademark holders.

Parody Web Sites

Ken Harvey was a speculator in domain names who lived in Newfoundland. Upon registering walmartcanadasucks.com and a number of similar domains, Ken created and uploaded a Web page stating that, "This is a freedom of information site set up for dissatisfied Wal-Mart Canada customers." The site exhorted visitors to "Spill Your Guts" with a "horror story relating to your dealings with Wal-Mart Canada." Wal-Mart responded by filing a complaint to a dispute-resolution provider, indicating that the domains were registered in bad faith. According to Wal-Mart, Ken's free speech argument was merely a cybersquatter's convenient and transparent dodge. On that basis, Wal-Mart sought to have control of the domain name walmartcanadasucks.com.

The dispute resolution provider held that Ken's conduct, even if distasteful, should not result in an unwarranted expansion of the domain name dispute process. According to the arbitrator, the dispute resolution process is meant to protect against trademark infringement, not provide a general remedy for all misconduct involving domain names. Having held that the walmartcanadasucks.com domain name is not identical or confusingly similar to Wal-Mart's trademarked name, the arbitrator decided that Ken did not register the domain name in bad faith. In fact, the arbitrator ruled that Ken had "a legitimate interest in respect of the domain name, to use it as a foundation for criticism of the complainant." On this basis, the request to transfer the domain name to Wal-Mart was refused.

Questions for Discussion

1. Should consumers be allowed to say whatever they want about a business, even if what they say is harmful and results in a loss of profits?
2. If you were the Wal-Mart executive charged with handling the matter, how might you have avoided arbitration?

Business Law in Action 17.1

Parody Web Sites

Ken Harvey was a speculator in domain names who lived in Newfoundland. Upon registering walmartcanadasucks.com and a number of similar domains, Ken created and uploaded a Web page stating that, "This is a freedom of information site set up for dissatisfied Wal-Mart Canada customers." The site exhorted visitors to "Spill Your Guts" with a "horror story relating to your dealings with Wal-Mart Canada." Wal-Mart responded by filing a complaint to a dispute-resolution provider, indicating that the domains were registered in bad faith. According to Wal-Mart, Ken’s free speech argument was merely a cybersquatter’s convenient and transparent dodge. On that basis, Wal-Mart sought to have control of the domain name walmartcanadasucks.com.

The dispute resolution provider held that Ken’s conduct, even if distasteful, should not result in an unwarranted expansion of the domain name dispute process. According to the arbitrator, the dispute resolution process is meant to protect against trademark infringement, not provide a general remedy for all misconduct involving domain names. Having held that the walmartcanadasucks.com domain name is not identical or confusingly similar to Wal-Mart’s trademarked name, the arbitrator decided that Ken did not register the domain name in bad faith. In fact, the arbitrator ruled that Ken had “a legitimate interest in respect of the domain name, to use it as a foundation for criticism of the complainant.” On this basis, the request to transfer the domain name to Wal-Mart was refused.

Questions for Discussion

1. Should consumers be allowed to say whatever they want about a business, even if what they say is harmful and results in a loss of profits?
2. If you were the Wal-Mart executive charged with handling the matter, how might you have avoided arbitration?

In some circumstances, the parties are entitled to litigate such matters. However, litigation requires a great deal of time and money to decide cases in the courts. Furthermore, because cybersquatting is a global activity, it is often difficult to decide which court should hear the matter. As a result, the bodies that regulate domain names have adopted procedures to resolve disputes primarily through arbitration. As we discussed in Chapter 1, arbitration is a form of alternative dispute resolution (or ADR) that allows the parties to settle their argument without a court order. As a matter of risk management, the best strategy is to avoid difficulties altogether. While that is not always possible, businesses can take steps to minimize the potential for domain name disputes. For instance, a business manager who is responsible for a company’s e-commerce development should register bona fide trademarks and business names as early as possible to avoid being held hostage by a cybersquatter. Note that even a registered trademark will not guarantee your business a proprietary interest in a particular domain name. Arbitrators have demonstrated a willingness to weigh the public interest in free speech and fair use against the rights of trademark holders.

Parody Web Sites

Ken Harvey was a speculator in domain names who lived in Newfoundland. Upon registering walmartcanadasucks.com and a number of similar domains, Ken created and uploaded a Web page stating that, "This is a freedom of information site set up for dissatisfied Wal-Mart Canada customers." The site exhorted visitors to "Spill Your Guts" with a “horror story relating to your dealings with Wal-Mart Canada.” Wal-Mart responded by filing a complaint to a dispute-resolution provider, indicating that the domains were registered in bad faith. According to Wal-Mart, Ken’s free speech argument was merely a cybersquatter’s convenient and transparent dodge. On that basis, Wal-Mart sought to have control of the domain name walmartcanadasucks.com.

The dispute resolution provider held that Ken’s conduct, even if distasteful, should not result in an unwarranted expansion of the domain name dispute process. According to the arbitrator, the dispute resolution process is meant to protect against trademark infringement, not provide a general remedy for all misconduct involving domain names. Having held that the walmartcanadasucks.com domain name is not identical or confusingly similar to Wal-Mart’s trademarked name, the arbitrator decided that Ken did not register the domain name in bad faith. In fact, the arbitrator ruled that Ken had “a legitimate interest in respect of the domain name, to use it as a foundation for criticism of the complainant.” On this basis, the request to transfer the domain name to Wal-Mart was refused.

Questions for Discussion

1. Should consumers be allowed to say whatever they want about a business, even if what they say is harmful and results in a loss of profits?
2. If you were the Wal-Mart executive charged with handling the matter, how might you have avoided arbitration?
INTERNET ACCESS PROVIDER AND ONLINE SERVICE PROVIDER LIABILITY

Problems cannot always be avoided, and disputes cannot always be settled through ADR. Litigation may be inevitable, especially if a business is engaged in global e-commerce. In that situation, it may not be enough to comply with local laws. Web site owners and operators must also consider the possibility of being dragged into court in some remote place. They must factor that possibility into the cost of doing business. And while it is expensive to ensure compliance in foreign legal systems, it is sometimes even more expensive to become embroiled in a far-away legal battle. Before considering compliance issues and the kinds of liability that might result from an electronic transaction, we need to first examine the question of jurisdiction.

Jurisdiction

Jurisdiction, in this context, refers to the ability of a court from a particular place to hear a case. Although the issue of jurisdiction can arise in any kind of case, it is particularly important for e-commerce disputes. Suppose that you have a company in British Columbia. That company has a registered trademark. You discover that a dot-com company in Saskatchewan that sells goods to people in Germany has improperly used your trademark on its Web site. That Web site is hosted by a server that is located in France. Where can you sue? British Columbia? Saskatchewan? France? Germany? At least three tests can be used to answer that question:

- a real and substantial connection test
- a passive versus active test
- an effects-based test

In Canada, the courts usually use a real and substantial connection test. They ask whether the plaintiff’s cause of action and the effects of the defendant’s conduct are sufficiently linked to the place in which the plaintiff wants to sue.27 Unfortunately, the courts are not yet sure how to apply that test in an e-commerce case. Early cases in the US likened the Internet to a continuous advertisement.28 On that basis, they said that information posted on a given Web site is directed to every place capable of accessing the site. Early decisions in Canada followed suit. For example, in Alteen v Informix, the defendant, an American manufacturer of information management hardware, allegedly issued untrue and misleading statements that led to an inflated stock price.29 When Newfoundland shareholders tried to sue, Informix argued that the Newfoundland court had no jurisdiction. Informix argued that it had no real and substantial connection to Canada as it did not trade shares on a Canadian stock exchange, never made press releases in Canada, and had no direct contacts with the plaintiffs. Still, the court held that the mere availability of the misleading statements on the Internet was sufficient to assert jurisdiction. Note that the effect of this approach is to potentially make every business liable for anything that it posts online.

27 Tolofson v Jensen (1994) 120 DLR (4th) 289 (SCC); Morguard Investments Ltd v De Savoye (1990) 76 DLR (4th) 256 (SCC).
Online business activity can take many forms, and the analogy between a Web site and a continuous advertisement is not always appropriate. Consequently, some courts now examine the online interaction to determine (i) the level of interactivity between the parties, and (ii) the commercial nature of the exchange of information that occurs on the Web site. Under this **passive versus active test**, a court looks at the way in which each party does business online. Is it merely posting information, or does it require customers to interact through the exchange of information online? Does its site send e-mail to particular places? Does it encourage customers from foreign places to call by providing a local or toll-free number? The more interactive a Web site is in a particular country, the more likely that a court in that country has jurisdiction to hear a case. There is an important point for risk management. If a company does not want to be involved in litigation in a particular place, it should avoid interacting online with people in that place. Case Brief 17.3 illustrates how a company can avoid the assertion of jurisdiction in places where it has no business.

More recently, several courts have moved away from a test that examines the specific characteristics, or the potential impact, of a particular Web site. Instead, they have adopted a broader **effects-based approach** that focuses on the actual impact a Web site has in the place where jurisdiction is being sought. To the extent that the courts are tempted to look at where the harm is done rather than how it is done, it will be very difficult for businesses to insulate themselves from possible liability in remote jurisdictions.

One way a business can protect itself is to avoid **targeting a location**. **Targeting a location** means specifically choosing to create relationships with people within that location. A business that targets individuals or corporations

---

**CASE BRIEF 17.3**


Desktop Technologies was the owner of the US federally registered trademark “Colorworks.” It came to Desktop’s attention that a Canadian company operating an identical kind of business not only used the same name as the mark (the Canadian company owned the Canadian trademark “ColorWorks”), it developed a Web site with the domain name www.colorworks.ca. That site contained several pages advertising ColorWorks services. The American company brought an action against the Canadian company in a Pennsylvania court.

The Canadian company had never done business or provided any of its services in Pennsylvania. It did business only in Canada. Though its Web site made available an online order form, it was purposely designed so that the form could not be filled out or sent via the Internet. To complete an order, the form had to be printed, filled out, and sent via fax or mail to Canada. Users were also provided with a telephone number in Canada as a point of contact.

After analyzing the commercial nature of the exchange of information that occurred on the Web site and the level of interactivity between the parties, the court held that every activity called for by the Web site was to take place in Canada. Consequently, the Web site functioned as little more than a passive form of advertising. Thus, the passive nature of the Web site was insufficient to permit the Pennsylvania court to exercise its jurisdiction over the defendant.

---


31. For an excellent legal and policy analysis of this approach, see M Geist “Is There a There There? Toward Greater Certainty for Internet Jurisdiction” (2001) Berkeley Tech LJ 1345.
within a particular place is more likely to have the courts there take its jurisdiction. There are a few things that a business can do to avoid targeting a jurisdiction.

- It can insert a jurisdictional clause into its standard form contract that requires any disputes arising from the agreement to be heard by the courts in a specified place. As we saw in our investigation of click-wrap and web-wrap contracts, such a clause will only be effective if adequate notice is given and if the other party is capable of assenting to it.
- A business can also use targeting technologies. Such technologies allow a company to manage the legal risks of e-commerce by restricting the geographical area in which it does business. You Be the Judge 17.1 illustrates this.

### Online Intermediaries

Online activity creates unique difficulties for jurisdictional issues. But for the most part, the threat of liability is much the same as it has always been. The tort of deceit, for instance, is identical whether it is committed in person by a con artist or over the Internet by a dot-con artist. However, electronic commerce may generate new forms of liability for certain kinds of online businesses, because of the role that online intermediaries play in various online relationships. An online intermediary is a party that enables or facilitates an online transaction between others. Think about all the things that need to happen before you can sell me stuff that is advertised on your Web site. First, someone has to agree to host your Web site. Second, unless I am fortunate enough to own an Internet server, someone needs to provide me with access to the Internet. I also need an e-mail account. So do you. Someone is probably in the business of storing or managing most of that data. There are, then, many kinds of busi-

---

**YOU BE THE JUDGE 17.1**

*UEIF et LICRA v Yahoo! Inc et Yahoo!France* 32

After viewing online auction sites that offered to sell thousands of Nazi objects (such as swastikas, daggers, uniforms and medals), two anti-racism groups based in Paris started an action against Yahoo! and Yahoo!France for "banalizing the Holocaust." Those groups demanded that Yahoo!France remove all hyperlinks to Yahoo!, which allowed Internet users to access racist material. Furthermore, these groups demanded that Yahoo!France explicitly warn its French users: (i) that Yahoo! contained racist content, and (ii) that they might break French law by browsing the U.S.-based search engine that contained racist materials.

Yahoo!France argued that its site was customized to be free of Nazi-related content and that the main Yahoo! site targeted a US audience, which protects the sale of Nazi objects as free speech. The French court nevertheless agreed with the plaintiffs. The court commissioned an independent international panel to determine whether technological means were available that would allow Yahoo! to continue to auction Nazi memorabilia in countries where it is legal to do so without targeting France. The panel reported that such technologies, though imperfect, are available. Consequently, the French court asserted jurisdiction and ordered Yahoo! to technologically avoid targeting the offensive auctions at France.

**Questions for Discussion**

1. Do you agree with the decision of the French court? Why?
2. What are some possible global ramifications of this decision?
3. If your managerial duties included overseeing a Web site that hosts online discussion, what changes might you make to the availability of your site in foreign jurisdictions?

---

32 Tribunal de Grande Instance de Paris (NRG 00/05308, 22 May 2000).
nesses that *intermediate* our transaction. They are all considered online intermediaries. In fact, you might even be one. If your business provides employees with access to the Internet or e-mail, then you are an online intermediary in any of their transactions. Here, we will focus on two different kinds of online intermediaries:

- Internet access providers
- Online service providers

**Internet Access Providers**

An **Internet access provider** provides others with access to the Internet. Suppose you start a business that provides Internet access for a flat fee. What happens if one of your customers uses your service to defame someone, download obscene materials, or breach copyright? As an intermediary, can you be held accountable? Generally speaking, the law says “no.” Internet access providers, like phone companies, are usually given special treatment, because they are in the business of supplying the pipeline, not monitoring its flow. That is not to say that an access provider is immune from all forms of liability. Suppose that you are an Internet access provider, and your standard contract absolutely guarantees customers uninterrupted service. One day, your service will go down. When it does, you will be liable for breach of contract. You could have avoided liability if you had anticipated service interruptions and provided for them in your standard contract. Or, suppose that you do not provide access for a fee, but for free to your employees. It is possible that they might do things online that attract liability to you as the access provider.33

**Online Service Providers**

Intermediary liability becomes much more difficult to determine in the context of **online service providers**. An **online service provider** offers goods or services, beyond mere Internet access, in exchange for something of value. Electronic commerce examples include e-mail suppliers, bulletin board operators, auction hosts, anonymous remailers, and commercial Web sites.

An online service provider usually enters into a contract with its subscriber. As usual, it can be held liable to that person if it breaches their agreement. However, it can also manage that risk by inserting an exclusion clause into the contract. Significantly, however, that strategy cannot protect an online service provider from liability to a third party. Since that party is not part of any contract and is therefore not bound by any exclusion clause, it may sue the service provider **as an intermediary**. For example, when a customer uses Yahoo! or AOL Canada to distribute a defamatory statement, the victim of that tort may sue both the customer and the online service provider. The victim may also sue the service provider for failing to reveal the true identity of the customer if that statement was posted under a false name. It is important to recognize, however, that you do not have to be an Internet giant to expose your business to these kinds of lawsuits. Risk managers will want to shield their online businesses against liability for: (i) posting defamatory remarks, (ii) distributing materials subject to copyright, (iii) disclosing personal information, (iv) trademark infringement, (v) computer mischief, and (vi) possession or distribution of child pornography, to name a few.

---

33. For example, an employee may download obscene materials in the workplace. By allowing the employee to create a hostile work environment, the employer may be held liable under human rights legislation, especially if the employer adopted a policy of monitoring employee conduct online but failed to enforce the policy.
The question of liability for online intermediaries is not perfectly settled. The confusion began with a pair of US decisions that reached opposite results on similar facts. In each case, an online intermediary hosted discussion boards that allowed members to speak freely on various controversial topics. In both cases, a subscriber to the online service posted defamatory remarks about a high-ranking member of a competing business. In both cases, the competing business sued the author of the remark and the online service provider who hosted the discussion. In both cases, the online service provider was in the business of hosting so many different discussion forums that it delegated the responsibility for maintenance and oversight of the discussion board in question to a subcontractor.

In each case, the court asked whether the service provider was a mere distributor, or whether it was a publisher, of the defamatory message. The distinction is crucial. A distributor is liable only if it actually knows that an illegal message was posted but does nothing about it. A publisher of an illegal message is liable in any event. In the first case, the court said that the online intermediary was a mere distributor and therefore not liable. But in the second case, the court held that the online service provider was liable as a publisher since it had exercised editorial control over the contents of its bulletin boards. Those two decisions suggest that service providers who exercise no editorial control over their sites are immune from liability, while service providers who exercise even a low level of control may be held liable.

The implications of those two decisions are troubling. Suppose that your Web site allows people to post messages. One user posts illegal materials that infringe someone's trademark or, worse still, contain violent pornography. If you monitor the site, see the illegal materials, and remove them, your decision to exercise editorial control might actually mean that you could be held liable for failing to remove other illegal postings that you missed or decided to not remove. Because you invoked editorial control, the law might treat you as a publisher. As you can see, there is a problem with using the element of editorial control to determine an online service provider's liability. Such a rule discourages service providers from monitoring their sites and removing offensive material.

In the United States and the United Kingdom, that problem has been addressed by legislation that protects online services providers from liability in some circumstances. Unfortunately, very few Canadian legislators have squarely addressed these issues. One province that has is Quebec. According to section 27 of its Act to Establish a Legal Framework for Information Technology, service providers acting as intermediaries are not required to monitor the information communicated on their networks or in the documents stored on them, nor are they required to report communications or documents that may be used for illegal activities. Even if a service provider chooses to monitor

34 Cubby Inc v CompuServe Inc 776 F Supp 135 (SDNY 1991); Stratton Oakmont v Prodigy Services Co WL 323710 (NY Sup Ct 1995).
35 In the US, the Communications Decency Act, 47 USC S 230(c) provides an extremely broad immunity: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” In the UK, a much more restricted immunity from liability is stipulated in section 1 of the Defamation Act, 1996 (UK) 1996 c 31: Applying this provision to the online environment, a service provider who: (i) is not an author; editor; or publisher; (ii) takes reasonable care, and (iii) does not know, or have reason to believe, that what they did caused or contributed to the publication of a defamatory statement, will be protected from liability for defamation.
37 Act to Establish a Legal Framework for Information Technology SQ 2001, c 32.
or report, its decision to do so will not automatically result in intermediary liability if illegal content is later found on its site. Section 36 of the Act states that service providers acting as intermediaries are not generally responsible for the illegal acts of service users. However, it also states that a service provider may incur liability if it participates in acts performed by service users.38

What about online service providers in other provinces? How can you shield your business from intermediary liability?

- You should have a clear contract with each user, possibly through a click-wrap agreement. Each user should be required to clearly consent to the terms of service that are contained in that contract. And those terms should allow you to claim indemnification from a user if you are ever held liable for something that they posted.39
- Those terms of service should clearly explain, with examples, which uses are acceptable and which are unacceptable.
- To avoid the risk of possible liability, you should, whenever possible, set up your business so that you can demonstrate that it merely acts as a conduit or pipeline for the materials that pass through the system.
- If you are sued, you should try to convince the court that while the legislation in Quebec, the US, and the UK are not binding in other places, they are based on policies that should be adopted.

### ONLINE CONSUMER PROTECTION

Electronic commerce can expose a business to risks other than legal liability. Many of these risks arise from a lack of caution and a dangerous tendency to trust strangers. Since many online business interactions do not take place in a secure environment and therefore lack the authentication procedures, consumers and small businesses often fall prey to the dot-cons. A dot-con is a con artist who has gone high-tech, using the Internet to defraud consumers.

One scam involves multi-level marketing. Multi-level marketing (MLM) is a system of marketing that puts more emphasis on recruiting distributors than on selling products. The dot-con sends an unsolicited message to a number of people, telling them all that they can get rich by joining its salesforce and recruiting others to do the same. Just as it gets paid by the people under it, the dot-con promises that the recruiters will also get paid by the people under them. Unfortunately, the products at the heart of the sales pyramid are usually overpriced, shoddy, and perhaps downright dangerous. And for every MLM distributor who makes a decent living or even a decent supplemental income, there are many more who pay more for their supplies and promotional materials than they will ever earn in sales. Given the nature of online interaction, MLMs are becoming more prevalent in electronic commerce. So are hosts of other online scams including: (i) duplicitous auctions, (ii) hidden-term contracts, (iii) forged invoices, (iv) deceptive advertising, (v) fraudulent credit card charges, (vi) fictitious business opportunities, and (vii) miracle cures.40

---

38. For example, liability may be imposed if the service provider: (i) sends a document, (ii) selects or alters the information in a document, (iii) determines who transmits, receives, or has access to a document, or (iv) stores a document longer than is necessary for its transmission.

39. Indemnification would require the user to compensate you for any losses that you suffered (for example, by being successfully sued as an intermediary by a third party).

Although business scams are as old as business itself, many con artists have begun to take advantage of high technology to peddle new and improved versions of traditional scams. We end this chapter with a brief look at consumer protection principles in the e-commerce environment. These principles are important to individuals as consumers; but they are also important to businesses. By adopting them, a business can enhance its reputation, strengthen consumer confidence, and ultimately increase sales.

Although some provinces have amended existing consumer protection legislation in light of electronic commerce, full-scale law reform has not yet occurred. Industry Canada promoted a set of guidelines in its Principles of Consumer Protection in Electronic Commerce: A Canadian Framework. However, those guidelines are not laws; they are simply suggestions for ethical and effective business practices that are intended to supplement the laws that already protect consumers. We summarize those guidelines.

1. Consumers should be provided with clear and sufficient information to make an informed choice about whether and how to make a purchase.

Online business should avoid jargon and use plain language whenever possible. They should clearly distinguish marketing and promotional material from the terms and conditions of sale. They should disclose the legal identity of their business, their business address, and any geographic limitations on where a product or service is for sale. They should fairly and accurately describe their goods. They should set out a complaints procedure and provide consumers with their own record of the transaction.

2. Vendors should take reasonable steps to ensure that the consumer’s agreement to contract is fully informed and intentional.

An online business should carefully set out the process of offer and acceptance. That process should require customers to confirm: (i) their interest in buying, (ii) the full price, terms and conditions, details of the order, and method of payment, and (iii) their agreement to purchase.

3. Vendors and intermediaries should respect privacy.

An online business should set up its data collection and information systems with a view to respecting and protecting its customers’ privacy.

4. Vendors and intermediaries should take reasonable steps to ensure that transactions in which they are involved are secure.

An online business should use the technology and procedures discussed in this chapter to safeguard payment and personal information that is exchanged or stored as a result of a transaction.

5. Consumers should have access to fair, timely, effective, and affordable means for resolving problems with any transaction.

An online business should have resources for handling consumer complaints efficiently and effectively. It should be aware that governments are working to clarify the rules governing online disputes, and to strengthen the enforceability of judgments, even in cross-border disputes.

---

6. **Consumers should be protected from unreasonable liability for payments in transactions.**

An online business should not charge people for unauthorized transactions, as when a third party uses a person’s credit information to purchase goods. If a person has already paid for an unauthorized transaction, the business should promptly provide a refund, even if the third party, who received the goods, cannot be found. Similarly, when a consumer mistakenly enters into a transaction, they should be allowed to cancel the agreement within a reasonable time. If a consumer disputes a sale because it did not receive adequate information about the relevant goods or services at the outset, the business should provide a refund, as long as the consumer returns the good or declines the service within a reasonable period of time.

7. **Vendors should not transmit commercial e-mail without the consent of consumers, or unless a vendor has an existing relationship with a consumer.**

Online businesses should avoid spamming, sending unsolicited e-mails to a large number of people. Not only is it bad netiquette, but spam exposes a business to the risk of being associated with products that are worthless, deceptive, and at least partly fraudulent. Many of the online scams that we discussed above are perpetrated through unsolicited mass e-mail. Why risk the reputation of your business when there are more sophisticated and successful means of advertising?

8. **Businesses should promote consumer awareness about the safe use of electronic commerce.**

A business’s goodwill is enhanced when it demonstrates a commitment to consumer education and awareness initiatives. An online business should therefore provide consumers with advice on how to minimize the risks associated with electronic commerce, explaining to them how best to conduct transactions safely and securely. When possible, consumers should be given access to information that identifies disreputable electronic commerce practices.

Business Decision 17.1 lets you reflect on the value of these guidelines.
Chapter Summary

Electronic commerce refers to technology-mediated business transactions. Although e-commerce has facilitated the development of the knowledge-based economy, its success will ultimately depend on eliminating various legal uncertainties and impediments.

Electronic commerce legislation seeks to enable online transactions by removing commercial uncertainty and other impediments. The co-ordination of model laws at both the international and national level has facilitated the global implementation of uniform laws at the provincial level. Canada’s model law, the Uniform Electronic Commerce Act, sets out a framework for inferring consent to participate in electronic transactions, the functional equivalents of paper-based requirements, the proper treatment of government documents, and a clarification of the rules of contract formation in the online setting (including the timing requirements for sending and receiving electronic documents). Although the adoption of electronic commerce in various Canadian jurisdictions differs in detail, many provinces and territories have maintained fidelity to much of the approach taken in UECA.

Online contracts, such as click-wrap and web-wrap agreements, have been recognized as enforceable provided the basic requirements of contract formation are adequately met. To ensure that an agreement is enforceable, managers charged with Web development should design online transactions with the requirements of electronic commerce legislation in mind. They should also ensure that the design of those transactions provides reasonable notice of the terms and conditions. Automated electronic commerce promises to dispense with the need for human supervision in the contract-formation process. Although most provincial legislation contemplates a method for rectifying keystroke errors, managers should incorporate safety mechanisms into their electronic contracts to protect their businesses against liability for computer-generated errors.

Public key infrastructure (PKI) promises to fortify the flimsy foundation of trust resulting from global online interaction. Information systems such as these can be used to authenticate transactions, ensure their integrity, and enhance online security. Technological measures are not, however, the sole means of ensuring information security. Business managers must also consider legal measures, including the adoption and enforcement of terms of service agreements and other strictly enforced corporate policies. A careful approach to information security will ultimately prove fundamental to the success of electronic commerce.

Although one key benefit of electronic commerce is that geography becomes less important, location is still relevant online. Domain names provide the virtual storefronts necessary for electronic commerce. Mimicking traditional real estate speculation, some individuals and companies are in the business of cybersquatting. Domain name registration authorities have developed uniform dispute resolution procedures to help resolve complaints brought by those claiming a proprietary interest in a particular domain name. For a fee, dispute resolution professionals will mediate and, if necessary, arbitrate disputes through various electronic media, thus decreasing the time and expense associated with traditional litigation.

The global reach of electronic commerce means that compliance with local laws is no longer sufficient insulation from legal risk. Web site owners and operators must consider the possibility that they may be dragged into a court battle in some remote jurisdiction. In resolving these disputes, Canadian courts consider whether there is a real and substantial connection between the cause of action, its effects, and the location in which the action has been commenced. Other considerations include the passivity or interactivity of the Web site and the actual effects of the alleged transgression in the location where jurisdiction has been sought. Targeting strategies, including the use of technological measures, will reduce the risk of being sued successfully in a foreign jurisdiction. The question of liability for online intermediaries is not perfectly settled. Early decisions have held that service providers who exercise no editorial control over their sites are immune from liability, whereas service providers who exercise even a low level of control might be held liable. Concerned that this approach provides a clear disincentive for service providers to read and remove illegal content from their Web sites, some jurisdictions have enacted legislation that provides a more balanced approach, extending further protection to online intermediaries under certain circumstances. The prospect of enhanced liability has led many Internet access and online service providers to insist on exclusion clauses in their terms of service. Prudent online intermediaries have also sought to implement practices to shield themselves from liability by demonstrating that they operate as mere conduits of electronic communication.

Full-scale law reform in the consumer protection area has not yet occurred. The most substantial development is a set of guidelines promoted by Industry Canada. Since these are not laws, any action taken by the Competition Bureau is merely educational in nature. Still, these guidelines offer insight to businesses and consumers about the shortcomings of conducting business online in a manner that does not ensure the development of trusting relationships with customers and clients.
Review Questions

1. In what sense is the law a source of uncertainty in the electronic commerce marketplace?

2. What are four potential benefits that electronic commerce offers to businesses willing to implement the use of information technologies?

3. What is the role and purpose of Canada’s Uniform Electronic Commerce Act?

4. How is Canada’s UECA enforced in each province and territory?

5. What are the relevant rules about sending and receiving electronic documents? As a risk manager, what steps can you take to avoid related disputes?

6. Given that electronic commerce legislation is provincially enacted, discuss several issues that a business manager should consider when engaged in interprovincial commerce.

7. Explain the difficulties associated with the formation of contracts online. What lesson can business managers learn from the case of Rudder v Microsoft?

8. How can information about products or services be designed to ensure that it is considered an invitation to treat? Why should a Web designer seek to do so?

9. Explain the complexities associated with automated electronic commerce. How can a business safeguard against the undesirable consequences of keystroke errors?

10. Explain how PKI is used for both security and authentication purposes. Why are the services of trusted third parties crucial to electronic commerce?

11. Summarize the process of cryptography. In what circumstances is public key cryptography preferable to private key cryptography? Explain.

12. How can businesses use the law as a deterrent to enhance information security? Provide two examples.

13. Distinguish between communications security and computer security, and provide an example of each.

14. What is cybersquatting? Is it ever legally permissible?

15. Describe three typical disputes arising from the domain name registration system, and provide an example of each. How can business managers avoid domain name disputes?

16. What factors should business managers consider when deciding whether to participate in electronic commerce on a global level? How can these risks be managed?

17. Name and discuss the variables that a court may consider in deciding if a specific online interaction falls under its jurisdiction.

18. Distinguish between online access providers and Internet service providers, and give an example of each. In which role is an online intermediary most likely to attract potential liability? Why?

19. As an online service provider in the province of Newfoundland, describe how you can shield yourself from possible liability as an online intermediary.

20. Describe how a business can incorporate consumer protection principles into its online contracting practices.

Cases and Problems

1. You are the general manager of a company that does business exclusively in Saskatchewan. With the aim of increasing efficiency and cutting costs, you are contemplating a change in corporate software that would enable filing all necessary government documents in electronic form. However, you are uncertain whether the provincial government will be obligated to accept documents in that form. Before paying a lawyer, you have decided to review the relevant legislation yourself to see if there is a clear answer. Using the legislation set out below, decide whether your company should switch to an electronic format. Can your provincial government force you to file solely by electronic means?

The Uniform Electronic Commerce Act contains these clauses concerning the filing of electronic forms with the government:

6. (1) Nothing in this Act requires a person to use or accept information in electronic form, but a person’s consent to do so may be inferred from the person’s conduct.

(2) Despite subsection (1), the consent of the Government to accept information in electronic form may not be inferred by its conduct but must be expressed by communication accessible to the public or to those likely to communicate with it for particular purposes.

9. A requirement under [enacting jurisdiction] law for a person to provide information to another person in a specified non-electronic form is satisfied by the provision of the information in an electronic document;

(a) if the information is provided in the same or sub-
2. As the president of a Web development company, you have been contacted by Alex Sadvar, the owner of the Naked Nature Art Studio. Alex wishes to revamp her Web site. Until now, the Web site functioned as a mere portfolio, inviting interested parties to contact her by telephone. Given her recent success and a seemingly never-ending demand for her drawings, she would like you to redesign her Web site so that it is capable of automated electronic commerce. As an astute business woman, Alex has expressed an interest in ensuring that the site’s design will protect her against erroneous customer orders. Prepare a proposal outlining how your Web design will take into account the relevant legislative provisions to minimize potential liability.

3. You are the information manager of an electronic mailing service BadNews.ca. Your primary customers are collections agencies. BadNews.ca assists these agencies by locating debtors and delivering legal notices to them before the repossession of their assets. You have been asked to determine the effect that the UECA will have on your company’s business practices. Prepare a brief memo explaining the rules governing the sending and receiving of electronic messages. Make sure that your memo provides some advice indicating the best way to avoid disputes with intended recipients.

4. Scroll Networks is a manufacturer of communications network hardware, including the XV11 routers used in wireless local area networks (LANs). ICanSolve Logistics Inc installs corporate LANs, purchasing its supplies directly from Scroll. Periodically, Scroll sends ICanSolve and other customers an electronic price list. When supplies are low, and the price looks right, ICanSolve often purchases 25 to 50 units of the XV11 router through Scroll’s online interface. During the course of Scroll’s online ordering process, the customer receives a click-wrap prompt requiring them to agree to the terms and conditions of sale. Among other provisions, they are advised in boldface red letters that prices are subject to change without notice at any time prior to shipment, and that “the seller is not liable for failure to deliver where materials are not reasonably available.” Additionally, the terms and conditions state that “acceptance of the order is expressly conditioned on the buyer’s assent to the seller’s terms and conditions.”

Upon obtaining inside information that XV11 router prices were scheduled to drastically increase the following day from $250 to $750 (due to a global shortage of integrated circuits), ICanSolve decided to place an order for 1000 XV11 routers. The following week, Scroll filled an order of 50 XV11 routers invoiced at $250 per unit. A letter accompanying the invoice stated that the enclosed portion of the order was priced at $250 as a gesture of goodwill but that the remaining 950 units would be priced at $750 per unit, due to the global shortage of integrated circuits. ICanSolve was offered 10 business days to cancel the balance of the order. ICanSolve accepted the initial delivery, but promptly contacted Scroll and demanded that the rest of the order be fulfilled at the advertised price. Scroll refused, arguing that its advertisements online and on paper indicated that the price was subject to change. What are the central legal issues in this case? How do you think that a court would resolve the dispute? If you were responsible for designing Scroll’s online interface, what might you have done differently to avoid situations like this?

5. Unlike most of your friends in business, you are quite
familiar with encryption technologies and have been using them for a few years. Recently, you have done further research on the use of trusted third parties in electronic commerce. In so doing, it has come to your attention that it is possible for a hacker to forge a pair of encryption keys, using them to deceive you into thinking that you have authenticated the sender’s identity when in fact you have not. Recognizing this possibility, you have decided to write a memo to the senior vice-president of your company explaining what a certification authority is and why your company should consider using one. Draft the memo.

6. Your company is drawing up an employee terms of service agreement. One paragraph states:

The computer network and connected devices are the property of the employer. The employer retains ownership and associated rights of all files, documents, and communications received, created, or stored by employees. The computer system is to be used for business purposes only. The e-mail system must not be used to transmit, view, or store obscene, defamatory, discriminatory, pornographic, threatening, sexually explicit, harassing, or any other offensive material. The e-mail system must not be used to duplicate or transmit copyright-protected material without the appropriate permission. At no time should confidential or trade secrets be transmitted over the Internet. The employer reserves the right to monitor e-mail communication and Internet browsing, and to make use of keystroke technologies at any time without notice. The employer retains the right to disclose an employee’s personal information, e-mail communication, and Internet browsing history upon request and without notice. Violation of this policy will result in employee discipline. By using the employer’s communication facilities, the employee acknowledges and consents to the above terms and conditions of usage.

Review this agreement. As a manager who is concerned about information security and intermediary liability, what is your opinion on its merits and shortcomings? What changes might be made to improve it?

7. Marcus is an employee of Scroll Networks. Alone at the office late one night with a pounding headache, deep concerns about meeting a deadline, and the knowledge that he was nowhere near finishing the assigned corporate memo, Marcus happened upon an idea. He decided that he would simulate a lightning strike on his company-issued laptop by stripping the Ethernet wire and inserting it into the 100 AC electrical wall outlet. Much to his surprise, he destroyed not only his laptop but also a cluster of workstations in the office. Although he stuck to his game plan, claiming that the office was struck by lightning, the hidden surveillance camera revealed otherwise. You are in charge of information security at Scroll Networks. What possible courses of action does the company have against Marcus? Assuming that you want to use the law as a means to educate employees at Scroll Networks and deter future information security breaches, which course of action will you choose, and why?

8. As the information manager of the XACTO Standard Weights and Measurements Corp, you have received an e-mail from a party identified as koko_k@pobox.com. The e-mail asks whether you are interested in purchasing the rights to the domain name www.xacto.ca. After entering the URL into your Web browser, you determine that the site is not currently in use. You then consult CIRA’s Web site and ascertain that the domain name was registered to a party named Koko Kerasic of Edmonton, Alberta only one week ago. Somewhat curious, you decide to respond to the koko_k e-mail, inquiring about the price. A reply to your e-mail comes only moments later demanding $75,000. As the person charged with overseeing your firm’s intellectual property enforcement, you are deeply concerned about securing that domain name.

You seek preliminary advice from your lawyer, Erik, who asks whether your company owns the Canadian trademark for XACTO. Your answer is “yes.” Erik then does a business search in Alberta to determine whether Koko has registered a business operating under the name XACTO. No such business name is registered. Upon further investigation, it turns out that Koko is an industrious 19-year-old high-school student who heard about cybersquatting in an ICQ chat room. Erik indicates that this matter must be resolved in accordance with the CIRA dispute resolution policy and quotes his fee for representing you in the matter. Given that your company is a financially-strapped startup, you decide to handle the matter without representation. You point your Internet browser to www.cira.ca and review the CIRA Domain Name Dispute Resolution Policy. What position will you take when making XACTO’s submissions to the CIRA dispute resolution provider? What argument can you expect from Koko or her parents? How is this matter likely to be resolved?

9. You are the owner of a small digital content provider based in Brandon, Manitoba. Your content is marketed under your Canadian registered trademark dFOX®. As well, you are the registered owner of the dFOX.com and dFOX.ca domain names. It has come to your attention that a US software company is advertising its newest voice-mailbot under the name dFOX on its Web site, codeworks.com. Code Works does not have a registered trademark for the dFOX product in the US or anywhere else. The Code Works site is targeted to Americans and explicitly warns that its voice-mailbot software may only work with US telecommunications hardware. The site has a US-only 1-888 number, but allows transactions to be completed online from anywhere in the world. The terms and conditions say that the warranty for the product is valid only for sales in the US. You decide to write a demand letter to Code Works, insisting that they cease using your trademark immediately. In the letter, you indicate that, for the past several weeks, customers confused by Code Work’s use of your mark have flooded your Web server, causing e-mail transmission problems and irreplaceable damage to some of your corporate hardware. Code Works ignores your demand and continues to market dFOX voice-mailbots on its Web site. You decide to go to a Manitoba court to seek a remedy for trademark infringement and economic loss. Outline the jurisdictional issues and tests you will be facing. What will your argument be? What can you expect Code Works to argue? As a risk manager, how can you seek to avoid legal liabilities in foreign jurisdictions?

10. You have decided to go into business as an online intermediary. Among other things, you maintain an online discussion board dedicated to financial issues and publicly-
traded companies. At times—especially when stock prices drop—conversation on the discussion boards heats up, and people start to point fingers. Sometimes inflammatory and demeaning remarks are made. To maintain community standards and keep the peace online, you have on occasion directed your Web master to remove certain remarks that you believe to be defamatory. Sometimes, the decision to remove such remarks results from your own random monitoring of the discussions. Other times, the decision results from requests or demands made by discussion board participants.

Today, you received a statement of claim alleging that you are liable for defamatory statements posted on your discussion board. The claim, filed by a large corporation and its CEO, is seeking millions of dollars in damages. This is the first that you have heard of any disparaging remarks made about that company. Although you have a policy to remove postings when asked, neither the corporation nor its CEO made any such request, and no one on your staff had noticed the remarks. Needless to say you are very concerned. You immediately check the discussion group and, sure enough, six false, disparaging remarks had been posted. After checking various financial records, you see that the complaining company’s stock prices plunged substantially the day after the remarks were made and have not since recovered. Is there any chance that the company might actually succeed against you? Explain why. How might a different approach to Web site management have reduced exposure to liability?

11. At a high-school reunion you run into an old classmate who has just returned from working in Malaysia. Upon hearing that you are now a renowned e-commerce entrepreneur, he corners you. After asking you several questions concerning online jurisdiction and consumer protection, he explains his latest business venture. It seems that he is marketing a cure for hair loss. According to him, he discovered the formula for a secret hair-regeneration tonic while working for a mining company deep in the heart of a rainforest. Apparently, the tonic can be manufactured from the ingredients found in the typical North American kitchen. He tries to recruit you to distribute his product online, promising you the recipe for the secret formula in exchange for a one-time payment along with a promise to buy a set quantity of promotional materials. To increase profits, you are also encouraged to recruit new distributors. Although your friend seems to be doing quite well for himself, as evidenced by the large diamond inlay in his gold tooth, you are suspicious. Could you be the target of a dot-com? Explain your reasoning.

12. The proliferation of electronic commerce has left consumer protection legislation slow to catch up. This has spurred Industry Canada to announce a policy that includes updated consumer protection principles tailored to the online environment. One of those principles is that, “Vendors should not transmit commercial e-mail without the consent of consumers, or unless a vendor has an existing relationship with a consumer.” If followed, would this principle always provide more protection to consumers? As a Canadian corporation, is your business required to adopt this policy? What are the likely business consequences of adopting it and the other principles announced by Industry Canada? What are the likely business consequences of ignoring them? Develop an appropriate e-mail business practice policy statement for your company.

Information as a Commodity

Intellectual Capital—Industry Canada
strategis.ic.gc.ca/SSG/pi00004e.html

This Web site provides information on current developments and intellectual capital through links to journal articles, research papers, and interviews.

Cognos
www.cognos.com/products/datamining.html

This software company offers data mining products and solutions to companies interested in transforming otherwise senseless business transaction information into extremely valuable assets.

Intellectual Property

Intellectual Property Policy Directorate—Industry Canada
strategis.ic.gc.ca/SSG/ip00001e.html

This directorate is responsible for reviewing and modernizing federal intellectual property laws. Its Web site provides news, research papers, laws and regulations, treaties, and links related to intellectual property.

Canadian Intellectual Property Laws and Regulations—Industry Canada
strategis.ic.gc.ca/SSG/ip01077e.html

This site provides links to the Canadian acts regulating patents, copyright, trademarks, industrial design, and integrated circuit topography.

Canadian Intellectual Property Office (CIPO/OPIC)
strategis.ic.gc.ca/sc_mrksv/cipo/welcome/welcome-e.html

The CIPO was created to administer the intellectual property system in Canada and provide information on intellectual property. Its Web site links to the Web pages of each subsection of intellectual property law.
World Intellectual Property Organization (WIPO)
www.wipo.org/index.html
This Web site provides information on intellectual property, WIPO activities and services, and links to treaties, decisions, and publications.

International Intellectual Property Treaties
strategis.ic.gc.ca/SSG/ip01076e.html
This Industry Canada Web page provides basic information on the international intellectual property treaties which Canada has signed and links to their full text.

Intellectual Property Institute of Canada (IPIC)
www.ipic.ca
The IPIC is a professional organization concerned with patents, trademarks, copyright, and industrial design. It maintains a list of intellectual property agents and lawyers.

Copyright Board of Canada
www.cb-cda.gc.ca
This site provides information on public hearings, recent decisions of the board, links to copyright collectives, and general information on copyright.

CANCOPY
www.uniquename.com/cancopy/home.html
Canadian creators and publishers established this not-for-profit agency to license public access to copyright works. Its site provides access to information on copyright licensing, an interface for affiliates and licensees, and resources relating to copyright.

Society of Composers, Authors and Music Publishers of Canada (SOCAN)
www.socan.ca
SOCAN collects and administers tariffs for music copyrights. Its Web site provides information on events, news, and other resources for both music users and music creators and publishers.

Recording Industry Association of America (RIAA)
www.riaa.org
RIAA represents the joint interests of many American film and music studios. Its site provides information on industry news, copyright, freedom of speech, licensing and royalties, piracy, audio technologies, and the interaction of music and the Internet.

US Copyright Office
lcweb.loc.gov/copyright
This US government Web site provides a wealth of US copyright information, publications, legislation, announcements, and a searchable registration database.

Canadian Trade-marks Database
strategis.ic.gc.ca/cgi-bin/sc_consul/trade-marks/search_e.pl
This online trademarks database allows you to search by trademark, status, application number, and registration number.

Canadian Trade-marks Journal
napoleon.ic.gc.ca/cipo/tradejournal.nsf/$$ViewTemplate+for+TMJournal+English?OpenForm
This CIPO Web page archives the Canadian Trade-marks Journal, which operates under the authority of the Trademark Act and publishes applications for trademarks for public comment and opposition.

Canadian Patent Database
patents1.ic.gc.ca/intro-e.html
This online searchable database lets you search, retrieve, and inspect over 1 400 000 patent documents in Canada, and European and US patents via a link to the World Intellectual Property Organization (WIPO).

US Patent and Trademark Office (USPTO)
www.uspto.gov
This US Department of Commerce site allows users to search patents and trademarks, order copies, apply for patents, register trademarks, pay fees, and monitor file progress.

PATSCAN—Patent and Trademark Searching
www.library.ubc.ca/patscan/welcome.html
This site provides patent and trademark searches for both university and industry, intellectual property resources, and database access.

Bizarre Patents—PATSCAN
www.library.ubc.ca/patscan/bizarre_patents.html
This page features the “bizarre patent of the month” and access to the PATSCAN archive of wacky patents.

International Chindogu Society
info.pitt.edu/~ctnst3/chindogu.html
Strange yet brilliant tools and devices.

Electronic Commerce
Electronic Commerce
aix1.uottawa.ca/~geist/ecommerce.html
This page provides a useful topical index to articles, case law, conferences, legislation, and policy papers on electronic commerce in Canada.

Electronic Commerce
canada.justice.gc.ca/en/ps/ec
The Department of Justice site addresses proposed
statutes on electronic commerce and provides links to news releases, consultation papers and reports, and other resources.

**Electronic Commerce Task Force**
e-com.ic.gc.ca/english/strat/641.html
This Industry Canada site offers information for companies involved in electronic commerce on marketplace rules—legal and commercial frameworks, financial issues and taxation, and intellectual property protection.

**Provincial Electronic Commerce Legislation and Regulation**
www.innovationlaw.org/lawforum/pages/ecommerce_legislation.htm
This site not only provides links to provincial electronic commerce legislation and regulations, but also offers background documents and links to other Internet-related legislation.

**Privacy Commissioner of Canada**
www.privcom.gc.ca/legislation/index_e.asp
This site provides links to Canadian privacy legislation, privacy guides, reference materials, and other privacy-related sites.

**The Validity and Enforceability of Web-wrap Agreements**
www.law.ualberta.ca/alri/ulc/current/ewebwrap.htm
This article examines the enforceability of online contracts with respect to traditional standard form contracts and fundamental contractual requirements.

**UNCITRAL Model Law on Electronic Signatures**
www.uncitral.org/english/workinggroups/wg_ec/wp-88e.pdf
This document contains a draft guide to the UNCITRAL Model Law on Electronic Signatures and provides insight into the principles of electronic signatures.

**Canadian Internet Registration Authority**
www.cira.ca
Operating as the authority for the registration of .ca domain names, this site also provides access to its official dispute resolution policy and rules.

**Institute for International Capital Research Inc.**
www.business.mcmaster.ca/mktg/nbontis/ic/
Used by both global organizations and governmental agencies, this institute offers consulting on knowledge management, intellectual capital, and organizational learning.

**Intangible Assets Manager**
This site offers a method for measuring intangible assets.